SAFFA: APLIKASI SISTEM DOKUMENTASI FORENSIK KOMPUTER

Adang Suhendra
Andreas Vangerow
Ayu Socanning Dyah
Fakultas Teknologi Industri, Universitas Gunadarma
Jl. Margonda Raya No. 100 depok
adang@staff.gunadarma.ac.id

ABSTRAK

Meningkatnya kejahatan yang berkaitan dengan teknologi menimbulkan adanya kebutuhan sistem yang dapat membantu menangani kejahatan khususnya yang memanfaatkan teknologi dalam hal ini teknologi komputer. Sistem dokumentasi hasil analisis uji forensik komputer membantu penyidik pada saat menyidangkan kasus kejahatan yang terkait dengan teknologi komputer. Tulisan ini menjelaskan pengembangan sistem dokumentasi forensik dinamakan SAFFA (Sistem Architecture For Forensic Analysis) yang disediakan dalam tiga bahasa yaitu Indonesia, Inggris, dan Jerman, serta diadaptasi agar dapat berjalan di berbagai sistem operasi. Sistem ini memfokuskan untuk analisis server dan komputer desktop. Sistem dapat memasukkan data hasil forensik dan menyimpannya dalam suatu basis data dengan struktur yang sesuai dengan standar dokumentasi data forensik.

***Kata kunci**: penyidik, kasus, kronologi*

PENDAHULUAN

Kemajuan teknologi Informasi ternyata tidak saja memberikan dampak positif tetapi juga sudah dimanfaatkan untuk melakukan kejahatan. Seperti beberapa kejadian pada beberapa tahun terakhir ini, peningkatan jumlah kejadian kejahatan cyber tumbuh seiring dengan kecepatan berkembangnya teknologi. Kejahatan cyber dapat didefinisikan sebagai kejahatan yang berhubungan dengan teknologi, komputer, dan internet (Techtv,2001).. Selanjutnya kejahatan cyber dapat pula disebut kejahatan komputer. Kerumitan dalam memberikan keputusan kejahatan komputer ini bisa memakan waktu berbulan-bulan atau bahkan bertahun-tahun bagi pengadilan untuk memutuskannya.

Ilmu forensik merupakan aplikasi ilmu dengan jangkauan yang luas, untuk menjawab pertanyaan yang berkaitan dengan sistem legal, bisa berkaitan dengan kejahatan atau dengan aksi sipil (Anonim). Definisi forensik komputer menurut Noblett adalah ilmu forensik untuk mengambil, menjaga, mengembalikan, dan menyajikan data yang telah diproses secara elektronik dan disimpan di media komputer (Anonim). Prioritas forensik komputer adalah untuk pemulihan dan analisis data. Tujuan forensik komputer adalah untuk mengamankan dan menganalisis bukti digital.

Dalam menindaklanjuti kasus kejahatan dengan komputer selain terdapat permasalahan dalam mengumpulkan dan menyajikan bukti-bukti yang diperlukan penyidik untuk memproses kasus kejahatan komputer, terdapat juga permasalahan lain yaitu dokumentasi hasil uji forensik komputer. Hal-hal yang didokumentasikan biasanya adalah manajemen bukti, segala hal yang berhubungan dengan kejahatan terkait termasuk pelaku, bagaimana, dan waktu kejadian. Tentu saja dengan demikian data yang ditangani dalam dokumentasi hasil uji forensik merupakan data yang besar dan kompleks.

Tulisan ini membahas tentang proses dokumentasi data hasil analisis

forensik komputer secara kronologis dan ditujukan untuk proses analisis forensik yang dikhususkan untuk komputer server dan desktop.

PEMBAHASAN

Forensik Komputer

Forensik komputer dapat didefinisikan sebagai ilmu forensik untuk mengambil, menjaga, mengembalikan, dan menyajikan data yang telah diproses secara elektronik dan disimpan di media komputer (Noblett). Definisi dari McKemmish menyebutkan bahwa forensik komputer adalah proses untuk mengidentifikasi, menjaga, menganalisis, dan menyajikan bukti digital dalam tata cara yang diterima secara hukum (Anonim) . Kedua definisi yang telah disebutkan, berprioritas pada penemuan kembali dan analisis data.

Pada definisi dari McKemmish diperkenalkan istilah bukti digital. Bukti digital sangat berkaitan dengan forensik komputer. Istilah bukti digital digunakan untuk menghindari keterbatasan yang ada pada istilah bukti elektronik (seperti bukti komputer, audio digital, video digital, telpon selular, mesin faks, dan lain-lain.)

Forensik komputer diterapkan pada penanganan kejahatan yang berkaitan dengan teknologi informasi. Forensik komputer dapat digunakan untuk menganalisis dan mengamankan bukti digital dan merupakan tata cara yang benar untuk menangani bukti digital. Kesulitan dalam forensik komputer adalah dalam menghadirkan bukti digital yang dapat digunakan dalam persidangan dan besarnya dokumentasi yang diperlukan. Sumber bukti digital (Geshonneck, 2006): Komputer desktop (menyimpan data catatan kegiatan pengguna, surat elektronik, dan lain-lain, dalam jumlah besar); sistem server (menyimpan data seperti komputer desktop tetapi untuk semua pengguna, dan berkas log lainnya); peralatan komunikasi, router atau modem (mengandung alamat IP, nomor telpon, dan lain-lain); lalu lintas komunikasi, surat elektronik, sesi penjelajahan situs, sesi transfer berkas, dan lain-lain; perangkat tertanam, sistem komputer kecil yang menjadi bagian dari sistem yang lebih besar; telpon bergerak, yang dapat menyimpan data seperti nomor telpon, pesan singkat, statistik panggilan, gambar, dan video.

Kesulitan yang dihadapi berkaitan dengan bukti digital (Anonim) mencakup kompleksitas, jumlah data yang besar, mudahnya bukti digital berubah (berubah di dalam komputer maupun pada jalur transmisi) tanpa meninggalkan jejak nyata, serta beragamnya teknologi informasi. Tingginya tingkat kompleksitas data terkadang mengakibatkan sulitnya pemahaman dalam proses analisis. Permasalahan besarnya ukuran jumlah data yang dianalisis memberikan ketidakefisienan dalam menganalisis data satu persatu sehingga teknik pengurangan data harus digunakan untuk memecahkan masalah ini.

Beberapa literatur menyebutkan bahwa prosedur forensik komputer yang perlu dilakukan oleh penyelidik terdiri dari: membuat salinan dari keseluruhan log data, berkass, dan lain lain yang dianggap perlu pada suatu media yang terpisah; membuat *sidik jari* dari data secara matematis (contoh : Hashing Algorithm, MD5), membuat sidik jari dari salinan secara matematis, membuat suatu Hashes *Masterlist*, dokumentasi yang baik dari segala sesuatu yang telah dikerjakan. Selain itu perlu dilakukan penyelidikan lebih lanjut, baik dengan menggunakan metode *search* dan *seizure* atau metode pencarian informasi. Penulisan ini lebih dititik beratkan pada langkah lima dalam prosedur forensik komputer yaitu langkah dokumentasi.

Dokumentasi Data Forensik

Sistem yang dikembangkan mendokumentasikan hasil analisis uji forensik komputer menggunakan alur kerja yang didokumentasi ke dalam beberapa text field yang berbeda pada sejumlah formulir. Formulir informasi hasil analisis dapat disimpan dan dibuka kembali oleh penyidik untuk proses lebih lanjut. Semua *text field* berkaitan dengan pertanyaan atau point tertentu yang berhubungan dengan analisis forensik dan sesuai dengan pedoman yang digunakan.

Adapun pedoman dokumen yang digunakan pada sistem ini adalah:

- A-SIT, *Secure Information Technology Center* (Austria) (Anonim) yang dikembangkan oleh *Austrian Federal Ministry of the Interior, National Specialist Law Enforcement Centre* (UK), *Federal Ministry of the Interior represented by the LKA Niedersachsen* (Germany), O.I.P.C.-INTERPOL *Sécreariat général*, EUROPOL, *National Criminal Investigation Department* (Sweden);*Seizure of e-evidence. Deliverable V1.01.* 15.12.2003. (rekomendasi dari *state offices of criminal investigation* Niedersachsen, Jerman.)
- U.S *Department of Justice. Office of Justice Programms. NIJ Special Report – Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* (Anonim, 2004;Anderson, 2006).
- ENFSI; *Guidelines For Best Practice in The Forensic Examination of Digital Technology* (rekomendasi dari *state offices of criminal investigation Niedersachsen*, Jerman.) (Anonim)
- Komputer-Forensik yang dikembangkan oleh Alexander Geschonneck (Geshonneck, 2006);

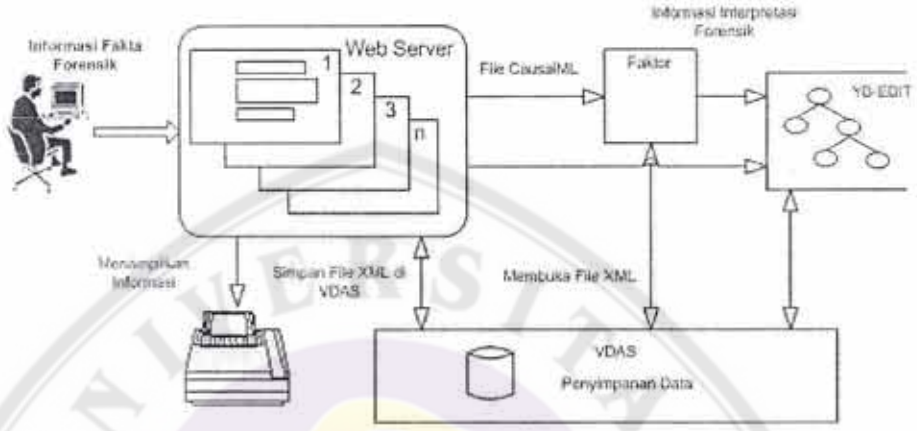
Sistem ini mendokumentasikan hasil analisis uji forensik komputer menggunakan aliran kerja yang terdiri dari beberapa text field yang berbeda pada sejumlah formulir (Gambar 1). Pada formulir tersebut informasi dari hasil analisis dapat disimpan dan jika analisis tersebut dibuka lagi penyelidik dapat memprosesnya lebih lanjut. Semua *text field* diperuntukkan bagi pertanyaan tertentu yang berhubungan dengan analisis forensik dan sesuai dengan pedoman yang digunakan. Titik tersebut diistilahkan sebagai indeks SAFFA. SAFFA terdiri dari 5 indeks dan beberapa sub indeks.

Hasil analisis dari perangkat lunak lain dapat dijadikan sebagai lampiran untuk pertanyaan atau point dari indeks yang berhubungan. Semua dokumentasi akan digabungkan dalam satu bungkus kejadian digital untuk setiap nomor kasus. Hasil analisis yang telah diinput akan disimpan pada sebuah berkas XML (Anonim, 2007) dengan nama sesuai dengan nomor kasus (nomorkasus.xml).

Bungkus kejadian digital berupa sebuah folder untuk setiap nomor kasus yang berbeda di dalam folder SAFFA-Archive. Nama folder ini sesuai dengan nomor kasus, di dalam folder ini disimpan berkas XML dan lampiran untuk setiap indeks. Untuk laporan forensik, SAFFA dapat mengubah berkas XML menjadi berkas HTML. Berkas HTML ini disimpan di dalam folder Bungkus kejadian digital dan dapat dicetak serta diedit pada aplikasi Ms Word atau OpenOffice. Selain itu dalam Bungkus kejadian digital disimpan juga folder untuk CausalMl. Dalam folder CausalMl akan disimpan berkas nomor kasus.xml dan nomorkasus.dot.

Sistem ini memungkinkan pengguna atau dalam hal ini penyelidik untuk membuat suatu interpretasi dengan dukungan metode formal untuk Causal Analysis (WBA). Penyelidik dapat menginput analisis WB untuk setiap point analisis. Bagian kanan tampilan halaman

analisis SAFFA diperuntukkan untuk analisis sistem causal. Dari analisis ini dapat dibuat sebuah "*list of facts*". List of fact digunakan untuk membuat suatu grafik analisis WB, grafik ini menunjukkan hubungan *causal* dalam bentuk diagram. Sebuah "fact" berisikan data mengenai indeks dan deskripsinya, daftar Necessary Causal Factor (NCF), jenisnya, dan lain-lain. Hasil analisis WBA inilah yang disimpan pada folder CausalML



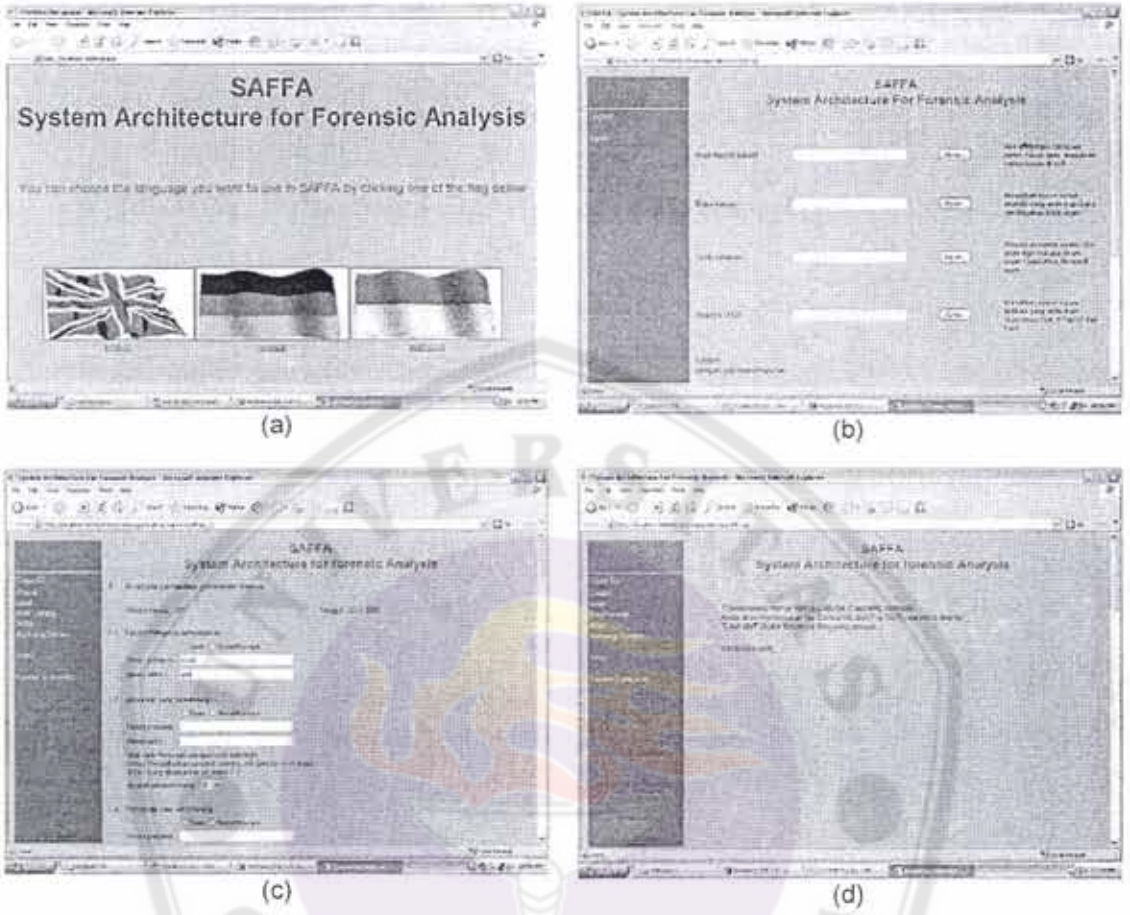
Gambar 1. Arsitektur Sistem Dokumentasi SAFFA

Rancangan Sistem dan Implementasi

Sistem yang dirancang terdiri dari lima proses, yaitu:

a. Pembuatan id kasus digunakan untuk memberikan nomor ID kasus baru. Kasus forensik akan dsimpan dalam format XML yang ditujukan agar mudah untuk diimplementasikan ke sistem lainnya.
b. Membuka ID kasus dimana sekaligus dapat menampilkan data forensik sesuai dengan ID kasus. Pengguna dapat melakukan perubahan data tersebut. Proses update akan dilakukan setelah proses validasi,
c. Menampilkan hasil uji forensik dalam bentuk format html. Berkas html yang telah dibuat dimasukkan dalam suatu Bungkus kejadian digital sesuai dengan ID khusus.
d. Analisis WBA (Why Because Analysis) memungkinkan pengguna untuk mendapatkan interpretasi dari setiap kasus.
e. Pengarsipan yaitu untuk mengambil dan menyimpan data kasus ke dalam sistem arsip.

Aplikasi dikembangkan menggunakan bahasa pemrograman Java dan JSP [5] untuk aplikasi webnya. Sistem ini tersedia dalam tiga bahasa yaitu Indonesia, Jerman dan Inggris. Gambar 2 adalah tampilan layar aplikasi yang dikembangkan, (a) merupakan menu utama; (b) tampilan pengisian data ID kasus; (c) melihat/mengubah data kasus forensik; (d) data sudah ditransformasikan ke untuk analiss WBA.



Gambar 2. Tampilan beberapa layar aplikasi

PENUTUP

Kesimpulan

Sistem dokumentasi hasil analisis uji forensik komputer (SAFFA) yang telah dapat menjadi suatu sistem dokumentasi hasil analisis forensic komputer yang kemudian dokumen tersebut dapat digunakan kembali untuk sistem lain karena disimpan dalam format XML yang diketahui memiliki sifat interoperabilitas. Dokumen XML data forensik ini kemudian dapat dilanjutkan dengan tahap analisis WBA dimana diketahui dapat membantu dalam penyelesaian penemuan bukti penyebab suatu kasus. Pemanfaatan teknologi XML ditujukan untuk memudahkan penggunaan oleh lingkungan yang lebih luas sehingga diharapkan dapat dikembangkan lebih lanjut. Sistem tersebut juga tersedia dalam tiga bahasa sehingga dapat digunakan lebih luas khususnya untuk Negara yang menggunakan tiga bahasa tadi..

DAFTAR PUSTAKA

Anonim. A-SIT, Secure Information Technology Center (Austria), http://www.a-sit.at/

_____ National Institute of Justice, US. Special Report – Forensic Examination of Digital Evidence: A Guide for Law Enforcement, April, 2004.

_____ ENFSI; Guidelines For Best Practice in The Forensic Examination of Digital Technoloy

_____ XML Extensible Markup Language, http:// www.w3.org/**XML**/, downloaded 2007

_____ Java Server Page Technology, http://java.sun.com/products/jsp/, downloaded 2007.

Anderson, Michael R, "Komputer Evidence Processing Good Documentation Is Essential",www.forensics-intl.com/art10.html, 6 juni 2006.

Geshonneck, Alexander, "Komputer-Forensik", dpunkt.verlag, 2006